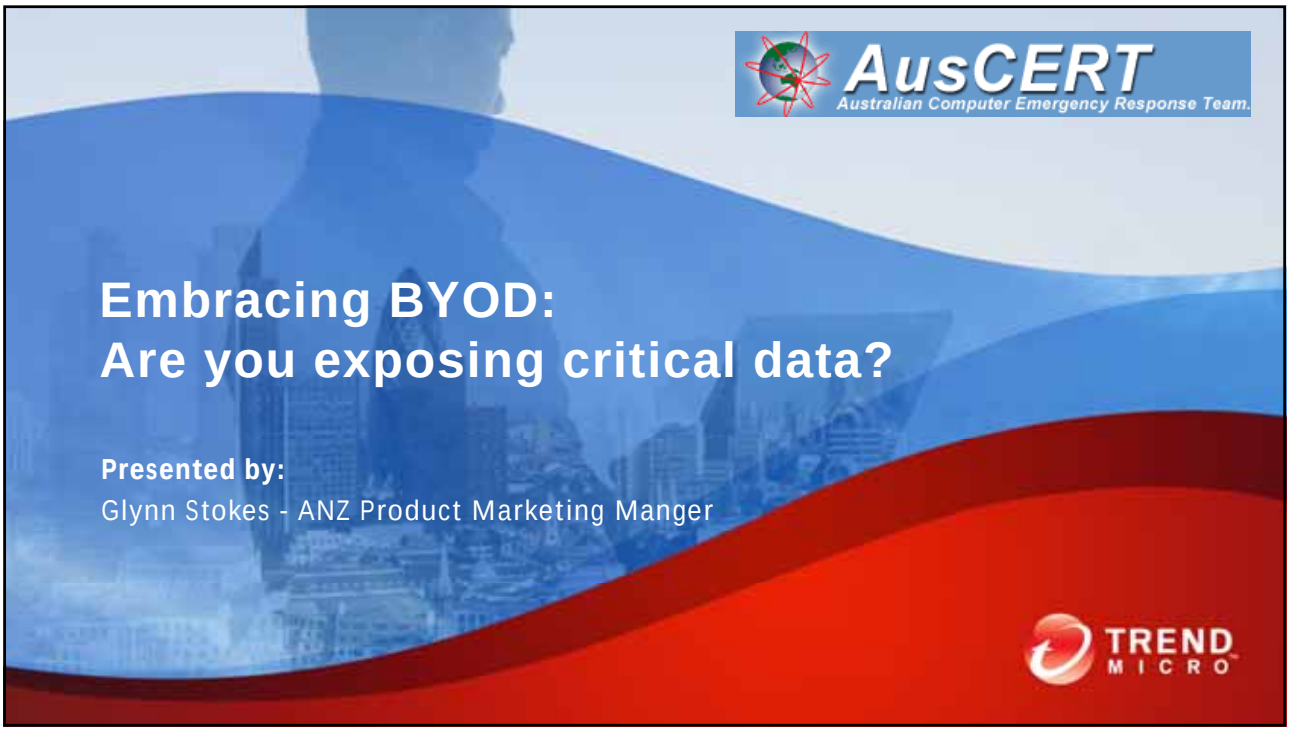
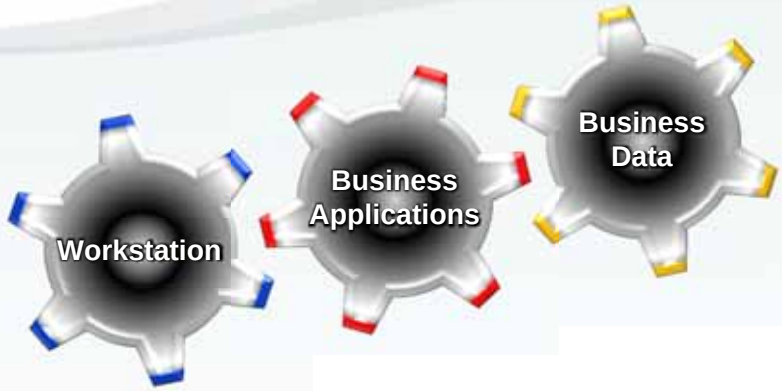


The Ever Changing Environment

We are experiencing the biggest change in the IT world since the invention of the Personal Computer!

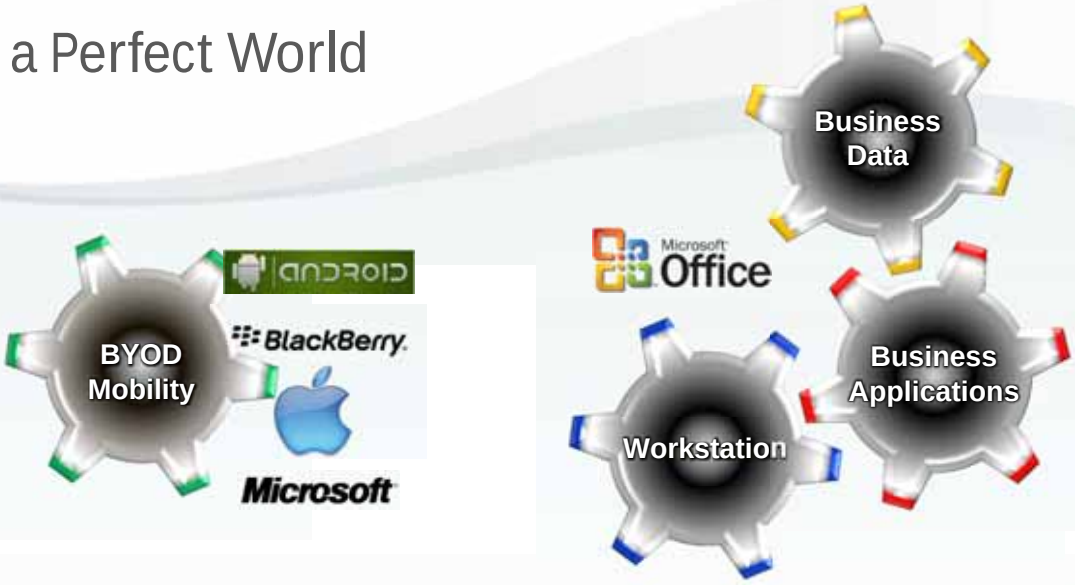
TREND MICRO

Traditional Business Environment



Traditional Business Environment

In a Perfect World



BYOD Questions

- What is a mobile device?

BYOD Questions

- Open or Closed Operating System?

Microsoft

android

Open systems provide access to the OS i.e. API etc
Easy access to applications – there are hundreds of Android App Stores.

BlackBerry

The Operating System is locked.
Applications only available via the Vendors App Store.
Vendor can remove apps from a device without the Users permission.
No Active X and Java Support.

TREND MICRO

BYOD Questions

- Specified or Unspecified Device?
  - Specified = Hardware Brand and OS Version
    - Example: Samsung Galaxy Running Android (Samsung Version)
  - Unspecified = ANY DEVICE

TREND MICRO

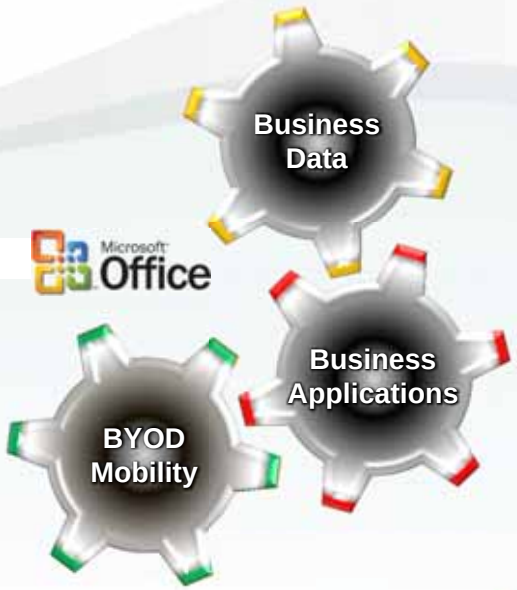
BYOD Questions

- To Manage or Not to Manage?
  - Specified is relatively easy.
  - Unspecified is NOT!.

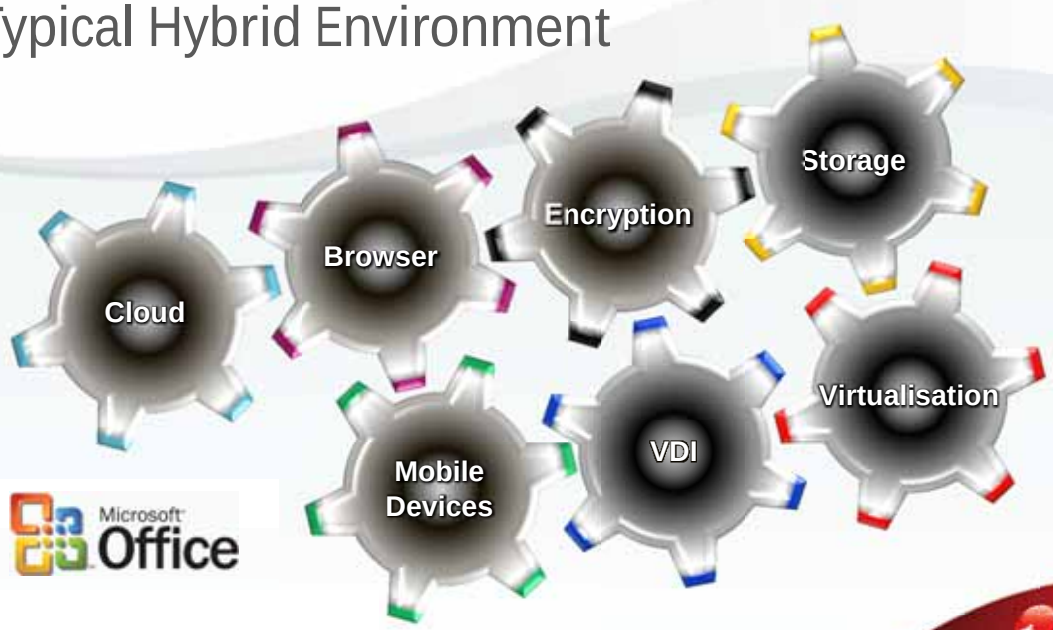
Other Considerations

- Access to business applications and data
  - What applications do they require in order to do their job and how do we deliver them?
- Business IP and Information
  - Where is my IP and Data located and how do I protect it?

A Solution



Typical Hybrid Environment

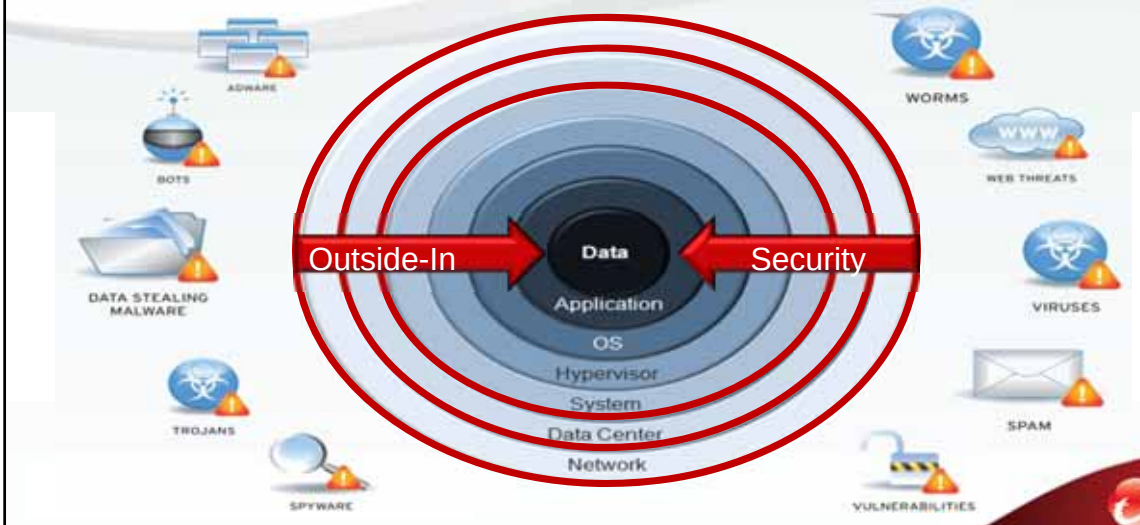


The Changing Environment

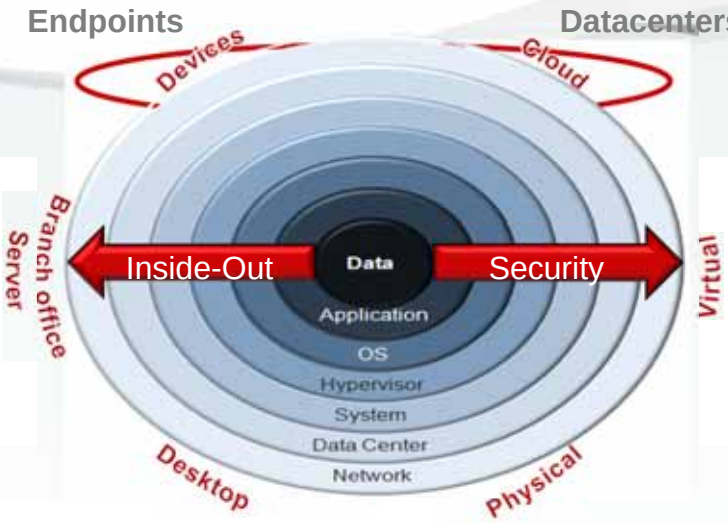
- "Traditional" and/or "edge" security creates new challenges
  - Vulnerabilities a constant headache
  - Virtualization and/or Cloud only increases complexity
  - Security profiles are decreasing
- A new security architecture is needed

The Outside-In Perimeter Defence Model

Layer protection from outside in keeps threats as far away as possible!



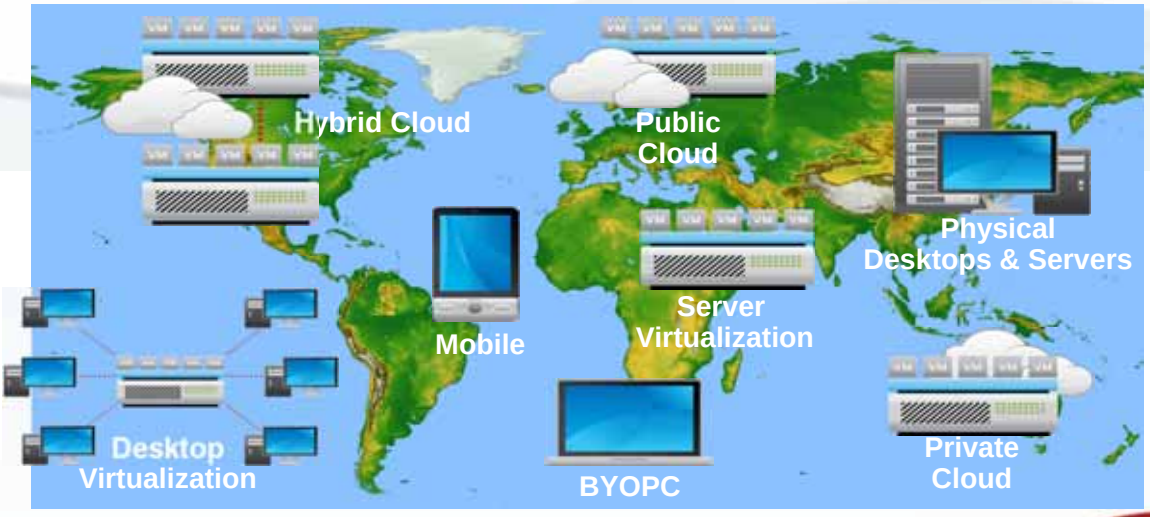
The Inside-Out Defence Model



All network-connected data must be able to defend itself from attacks

15

Protecting your IP and Data – Where is it?



16

Protecting your IP and Data

- You need to be able to protect your IP and Data no matter where its is located.
- Or Control where it can be located.
- You need to protect the Work Process and Data not the just the system.

Encryption

- The only real way to insure that your data is protected no matter where it is located.
- You must control the….
  - Keys
  - Who has the ability to see the data
  - Ability to wipe the data should a device be lost.

Protecting the VDI

- If you do not know the security posture of a BYO device then you need maximum protection on the VDI.
- Not just Anti-malware but Host Intrusion Prevention including Vulnerability Shielding.
- Limit what the VDI can do.

Summary

- Need to balance the risk vs the reward that BYOD provides.
- Protect your Data and it should be able to defend itself from attack.
- More than just Anti-malware protection.
- Where possible you need to be in control.


AusCERT
Australian Computer Emergency Response Team.
Thank You
TREND MICRO